

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

IN RE APPLICATION OF: Akihiko SUGIKAWA

GAU:

SERIAL NO: New Application

EXAMINER:

FILED: Herewith

FOR: WIRELESS COMMUNICATION DEVICE, PORTABLE TERMINAL, COMMUNICATION CONTROL
PROGRAM AND COMMUNICATION SYSTEM

REQUEST FOR PRIORITY

COMMISSIONER FOR PATENTS
ALEXANDRIA, VIRGINIA 22313

SIR:

Full benefit of the filing date of U.S. Application Serial Number , filed , is claimed pursuant to the provisions of 35 U.S.C. §120.

Full benefit of the filing date(s) of U.S. Provisional Application(s) is claimed pursuant to the provisions of 35 U.S.C. §119(e). Application No. Date Filed

Applicants claim any right to priority from any earlier filed applications to which they may be entitled pursuant to the provisions of 35 U.S.C. §119, as noted below.

In the matter of the above-identified application for patent, notice is hereby given that the applicants claim as priority:

<u>COUNTRY</u>	<u>APPLICATION NUMBER</u>	<u>MONTH/DAY/YEAR</u>
Japan	2002-321348	November 5, 2002

Certified copies of the corresponding Convention Application(s)

are submitted herewith

will be submitted prior to payment of the Final Fee

were filed in prior application Serial No. filed

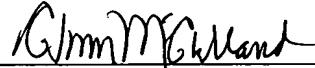
were submitted to the International Bureau in PCT Application Number
Receipt of the certified copies by the International Bureau in a timely manner under PCT Rule 17.1(a) has been acknowledged as evidenced by the attached PCT/IB/304.

(A) Application Serial No.(s) were filed in prior application Serial No. filed ; and

(B) Application Serial No.(s)
 are submitted herewith
 will be submitted prior to payment of the Final Fee

Respectfully Submitted,

OBLON, SPIVAK, McCLELLAND,
MAIER & NEUSTADT, P.C.



Marvin J. Spivak

Registration No. 24,913

C. Irvin McClelland
Registration Number 21,124

Customer Number

22850

Tel. (703) 413-3000
Fax. (703) 413-2220
(OSMMN 05/03)

日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されて
いる事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed
with this Office.

出願年月日 2002年11月 5日
Date of Application:

出願番号 特願2002-321348
Application Number:

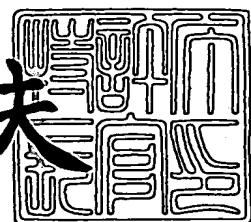
[ST. 10/C] : [JP2002-321348]

出願人 株式会社東芝
Applicant(s):

2003年 7月18日

特許庁長官
Commissioner,
Japan Patent Office

今井康夫



【書類名】 特許願
【整理番号】 13942301
【提出日】 平成14年11月 5日
【あて先】 特許庁長官殿
【国際特許分類】 H04B 7/00
【発明の名称】 近接通信装置、携帯端末、近接通信装置を制御するプログラム、携帯端末を制御するプログラム及び通信システム
【請求項の数】 13
【発明者】
【住所又は居所】 神奈川県川崎市幸区小向東芝町1番地 株式会社東芝
研究開発センター内
【氏名】 杉 川 明 彦
【特許出願人】
【識別番号】 000003078
【住所又は居所】 東京都港区芝浦一丁目1番1号
【氏名又は名称】 株式会社 東 芝
【代理人】
【識別番号】 100075812
【弁理士】
【氏名又は名称】 吉 武 賢 次
【選任した代理人】
【識別番号】 100088889
【弁理士】
【氏名又は名称】 橋 谷 英 俊
【選任した代理人】
【識別番号】 100082991
【弁理士】
【氏名又は名称】 佐 藤 泰 和

【選任した代理人】

【識別番号】 100096921

【弁理士】

【氏名又は名称】 吉 元 弘

【選任した代理人】

【識別番号】 100103263

【弁理士】

【氏名又は名称】 川 崎 康

【手数料の表示】

【予納台帳番号】 087654

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 近接通信装置、携帯端末、近接通信装置を制御するプログラム、携帯端末を制御するプログラム及び通信システム

【特許請求の範囲】

【請求項 1】

所定の範囲内に位置する他の通信装置との間で通信を行うことが可能な近接通信手段を備えた近接通信装置において、

自装置を識別するための自装置情報を取得する自装置情報取得手段と、

自装置が提供するサービス名称と前記自装置情報を含む第1識別情報を生成する第1識別情報生成手段と、

予め定めた暗号鍵を用いて前記第1識別情報を暗号化して暗号化データを生成する暗号化手段と、

前記サービス名称、前記自装置情報及び前記暗号化データを含む第2識別情報を生成する第2識別情報生成手段と、

前記自装置情報の送信要求を行った他の通信装置に対して、前記第2識別情報を送信する自装置情報送信手段と、を備えることを特徴とする近接通信装置。

【請求項 2】

前記第1識別情報生成手段は、前記サービス名称と前記自装置情報を合わせたデータに対してハッシュ演算を行って得られたハッシュ値を前記第1識別情報とすることを特徴とする請求項1に記載の近接通信装置。

【請求項 3】

前記第2識別情報生成手段は、前記サービス名称の後に続けて前記暗号化データを配置し、前記サービス名称の前に、前記サービス名称の長さを示す情報を配置した前記第2識別情報を生成することを特徴とする請求項1または2に記載の近接通信装置。

【請求項 4】

前記第2識別情報生成手段は、前記サービス名称の長さを示す情報の前に、高速処理を指示する情報を配置した前記第2識別情報を生成することを特徴とする請求項3に記載の近接通信装置。

【請求項 5】

前記近接通信手段は、Bluetoothの仕様で通信を行い、

前記自装置情報は、Bluetoothアドレスであることを特徴とする請求項1及至4のいずれかに記載の近接通信装置。

【請求項 6】

所定の範囲内に位置する他の通信装置との間で通信を行うことが可能な近接通信手段を備えた携帯端末において、

自端末と通信可能な通信装置を探索する探索手段と、

前記探索された通信装置から送信された第1識別情報を取得する識別情報取得手段と、

前記取得された第1識別情報から、サービス名称、自装置情報及び暗号化データを抽出する情報抽出手段と、

予め定めた解読鍵を用いて、前記暗号化データを復号する復号手段と、

前記復号されたデータと、前記情報抽出手段で抽出されたサービス名称及び自装置情報とを比較し、前記探索手段で探索された通信装置が信頼できるか否かを判定する比較判定手段と、

前記比較判定手段により信頼できないと判定された通信装置との通信を禁止する通信制御手段と、を備えることを特徴とする携帯端末。

【請求項 7】

前記比較判定手段により信頼できないと判定された通信装置に利用者が接続しようとした場合に、信頼できないことを示す情報を利用者に提示する情報提示手段を備えることを特徴とする請求項6に記載の携帯端末。

【請求項 8】

前記比較判定手段により信頼できないと判定された通信装置の一覧を登録するリスト登録手段を備え、

前記通信制御手段は、前記リスト登録手段に登録されている通信装置との通信を禁止することを特徴とする請求項7に記載の携帯端末。

【請求項 9】

前記情報抽出手段で抽出されたサービス名称及び装置識別名称をあわせたデータ

タに対してハッシュ演算を行ってハッシュ値を生成するハッシュ演算手段を備え

前記比較判定手段は、前記復号されたデータと前記生成されたハッシュ値とを比較することを特徴とする請求項6及至8のいずれかに記載の携帯端末。

【請求項10】

前記近接通信手段は、Bluetoothの仕様で通信を行い、

前記自装置情報は、Bluetoothアドレスであることを特徴とする請求項6及至9のいずれかに記載の携帯端末。

【請求項11】

所定の範囲内に位置する他の通信装置との間で通信を行うことが可能な近接通信手段を備えた近接通信装置を制御するコンピュータ読み取り可能なプログラムにおいて、

自装置を識別するための自装置情報を取得するステップと、

自装置が提供するサービス名称と前記自装置情報を含む第1識別情報を生成するステップと、

予め定めた暗号鍵を用いて前記第1識別情報を暗号化して暗号化データを生成するステップと、

前記サービス名称、前記自装置情報及び前記暗号化データを含む第2識別情報を生成するステップと、

前記自装置情報の送信要求を行った他の通信装置に対して、前記第2識別情報を送信するステップと、を備えることを特徴とする近接通信装置を制御するプログラム。

【請求項12】

所定の範囲内に位置する他の通信装置との間で通信を行うことが可能な近接通信手段を備えた携帯端末を制御するコンピュータ読み取り可能なプログラムにおいて、

自端末と通信可能な通信装置を探索するステップと、

前記探索された通信装置から送信された第1識別情報を取得するステップと、

前記取得された第1識別情報から、サービス名称、自装置情報及び暗号化データ

タを抽出するステップと、

予め定めた解読鍵を用いて、前記暗号化データを復号するステップと、

前記復号されたデータと、前抽出されたサービス名称及び自装置情報とを比較し、前記探索された通信装置が信頼できるか否かを判定するステップと、

信頼できないと判定された通信装置との通信を禁止するステップと、を備えることを特徴とする携帯端末を制御するプログラム。

【請求項 13】

携帯端末と、所定の範囲内に位置する前記携帯端末との間で通信を行うことが可能な近接通信手段と、を備えた通信システムにおいて、

前記携帯端末は、

自端末と通信可能な通信装置を探索する探索手段と、

前記探索された通信装置から送信された第1識別情報を取得する識別情報取得手段と、

前記取得された第1識別情報から、サービス名称、自装置情報及び暗号化データを抽出する情報抽出手段と、

予め定めた解読鍵を用いて、前記暗号化データを復号する復号手段と、

前記復号されたデータと、前記情報抽出手段で抽出されたサービス名称及び自装置情報とを比較し、前記探索手段で探索された通信装置が信頼できるか否かを判定する比較判定手段と、

前記比較判定手段により信頼できないと判定された通信装置との通信を禁止する通信制御手段と、を有し、

前記近接通信装置は、

自装置を識別するための自装置情報を取得する自装置情報取得手段と、

自装置が提供するサービス名称と前記自装置情報とを含む第1識別情報を生成する第1識別情報生成手段と、

予め定めた暗号鍵を用いて前記第1識別情報を暗号化して暗号化データを生成する暗号化手段と、

前記サービス名称、前記自装置情報及び前記暗号化データを含む第2識別情報を生成する第2識別情報生成手段と、

前記自装置情報の送信要求を行った他の通信装置に対して、前記第2識別情報を送信する自装置情報送信手段と、を有することを特徴とする通信システム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、Bluetoothなどの比較的狭い範囲で通信を行う近接通信装置と、この種の近接通信装置と通信を行う携帯端末とに関する。

【0002】

【従来の技術】

最近、伝送距離が10m程度の近距離無線通信方式が注目を集めている。従来の無線LANの有効な伝送距離範囲が100m以上であるのに対し、近距離無線通信方式は、伝送範囲が狭い分、使用する電力が少ないので、携帯電話やPDA等の携帯型情報処理装置（以下、簡単に携帯端末と呼ぶ）などのバッテリーに制限がある情報処理装置に適している。

【0003】

Bluetooth（登録商標）は、このような近距離無線通信方式の1つであり、近年、このBluetooth通信機能を備えた携帯端末が普及し始めている（非特許文献1参照）。

【0004】

Bluetoothは、デバイスの単価が安くて装置の小型化が可能なため、Bluetooth通信機能を備えた装置が今後いたるところに普及すると予想される。Bluetoothの普及により、任意の場所で、各場所に応じたサービスや情報を提供できるようになる。

【0005】

例えば、コンビニエンスストア、スーパー及び小売店などでは、電子クーポンサービス、電子ポイントサービス、電子決済、レシート及び領収書発行などの購買者向けのサービスを行うことができる。また、電子チケットによるゲート開閉の制御、自動販売機での決済や割引サービス、駐車場、ガソリンスタンド及びドライバースルーでの料金支払いなどへの応用が期待されている。この他、インターネ

ットへのアクセス、情報配信及び位置情報の提供なども可能になる。特に、人が多く集まるような駅や待ち合わせのスポットには、Bluetooth通信機能を備えた数多くの装置が設置されることが予想される。

【0006】

以下、Bluetooth通信機能を備えた携帯端末（以下、簡単にBluetooth端末と呼ぶ）と、Bluetooth通信機能を備えて各種サービスを提供する情報処理装置（以下、簡単にBluetooth装置と呼ぶ）との間で、Bluetoothによる接続を確立し、当該Bluetooth端末を所持するユーザにBluetooth装置がサービスを提供する場合を例にとって、従来技術を説明する。

【0007】

まず、Bluetooth端末が任意の場所で任意の相手からサービスを受けるための手順を説明する。図8はこの手順を示すフローチャートである。まず、サービスを受けるためのアプリケーションを起動する（ステップS1）。次に、Bluetooth端末は、インクワイアリを行って周囲の通信可能な端末の発見を試みる（ステップS3）。

【0008】

次に、Bluetooth端末は、発見した端末のリモートネームを取得する（ステップS4）。次に、一定時間経過後、インクワイアリが完了すると、Bluetooth端末は、インクワイアリで発見した装置のリモートネームの一覧を利用者に提示する（ステップS5）。

【0009】

次に、Bluetooth端末は、利用者が選択したBluetooth装置に対してACL接続要求を行う（ステップS6）。そして、ACL接続完了後、Bluetooth端末は、サービス情報取得コマンドを送信する（ステップS7）。

【0010】

次に、Bluetooth端末は、サービス情報を取得し、アプリケーションが利用するプロファイルをサポートしているか検査する（ステップS8）。プロファイルをサポートしている場合は、Bluetooth端末は、そのプロファイルに関する接続情報を取得する（ステップS9）。

【0011】

Bluetooth端末は、取得した情報を用いてそのプロファイルに対して接続要求を行う（ステップS10）。プロファイルの接続完了後、Bluetooth端末は、アプリケーションレベルでサーバ認証を行う（ステップS11）。

【0012】

以上の手順により、利用者は、Bluetooth端末を使用して所望のサービスを受けることが可能となる。

【0013】**【特許文献1】**

特開2002-152196公報（←ハッシュデータ比較によるプログラムID認証）

【非特許文献1】

Member Web Site、“Specifications”他、[online]、The Bluetooth SIG, Inc.、[平成14年10月29日検索]、インターネット<URL: <http://www.bluetooth.org>>

【0014】**【発明が解決しようとする課題】**

ここで、Bluetoothを使用したサービスや情報提供装置が普及し、公衆の集まる駅やスポットにBluetooth装置が多数配置された状況での使用を想定して説明する。特に人の多く集まるような場所では、有益な情報ばかりでなく、多くの人に無益の情報（ローン、アダルト情報、ギャンブル等）も多数配信されることが容易に想像できる。

【0015】

このような状況で、サービスや情報を取得しようとして、Bluetooth端末から通信可能なBluetooth装置の発見を試みると、有益無益にかかわらず多くのBluetooth装置が発見されることとなる。

【0016】

現状では、インクワイアリで取得できる情報に含まれるBluetooth装置の種類に関する情報を記したCOD(Class of Device)を用いれば、所望のサービスを提供

するBluetooth装置のみを絞り込むことができる。

【0017】

しかし、CODは、装置の種類であってサービスそのものを識別しているのではない。例えば、CODに情報配信装置のカテゴリーがあったとしても、それが、どのような情報を配信する装置かをCODのみでは識別できず、リモートネームで相手装置の名前を取得して初めてわかることがある。

【0018】

ところが、リモートネームは容易に設定できるため、その装置が本当にそのサービスや情報を提供しているかは、サービス提供を行うプロファイル、例えば、FTPプロファイルの接続を行い、実際に情報を取得しなければわからない。

【0019】

特定の情報を取得するための専用のアプリケーションを使用するのであれば、例えば、居酒屋情報が欲しい場合は、そのアプリケーションにあらかじめ居酒屋情報提供装置に共通な鍵を持たせておき、Bluetoothのリンク認証機構、あるいは、OBEXの相手認証機能を用いることにより、偽者の装置に接続することを防ぐことができる。

【0020】

ただし、Bluetoothリンク認証やOBEXの認証も、利用者がその装置に接続を行うまで、正しい装置かどうか確認できないため、無益な情報を提供する装置が多数存在すると、利用者が本来必要とするサービスや情報取得にかかる時間や手間が増えてしまう。

【0021】

また、リモートネームに利用者の興味をひく宣伝文だけを埋め込んでおいた場合、利用者が通信可能な装置を探索したときに、その宣伝文句を目にするになり、利用者が希望する端末の選択を阻害することとなる。

【0022】

リモートネームは容易に設定できるため、その装置が利用者の所望のサービスや情報を本当にサポートしているかは、接続してみて実際に確認しなければならず、利用者に余分な時間や労力をかけることとなる。

【0023】

また、リモートネームに宣伝文句が設定された装置が存在すると、利用者が接続を希望する装置の選択を大きく阻害してしまう。

【0024】

本発明は、このような点に鑑みてなされたものであり、その目的は、信頼できるサービスを提供する通信装置に簡易かつ迅速かつ正しく接続可能な近接通信装置、携帯端末、近接通信装置を制御するプログラム及び携帯端末を制御するプログラムを提供することにある。

【0025】**【課題を解決するための手段】**

上述した課題を解決するために、本発明は、所定の範囲内に位置する他の通信装置との間で通信を行うことが可能な近接通信手段を備えた近接通信装置において、自装置を識別するための自装置情報を取得する自装置情報取得手段と、自装置が提供するサービス名称と前記自装置情報を含む第1識別情報を生成する第1識別情報生成手段と、予め定めた暗号鍵を用いて前記第1識別情報を暗号化して暗号化データを生成する暗号化手段と、前記サービス名称、前記自装置情報及び前記暗号化データを含む第2識別情報を生成する第2識別情報生成手段と、前記自装置情報の送信要求を行った他の通信装置に対して、前記第2識別情報を送信する自装置情報送信手段と、を備える。

【0026】

また、所定の範囲内に位置する他の通信装置との間で通信を行うことが可能な近接通信手段を備えた携帯端末において、自端末と通信可能な通信装置を探索する探索手段と、前記探索された通信装置から送信された第1識別情報を取得する識別情報取得手段と、前記取得された第1識別情報から、サービス名称、自装置情報及び暗号化データを抽出する情報抽出手段と、予め定めた解読鍵を用いて、前記暗号化データを復号する復号手段と、前記復号されたデータと、前記情報抽出手段で抽出されたサービス名称及び自装置情報を比較し、前記探索手段で探索された通信装置が信頼できるか否かを判定する比較判定手段と、前記比較判定手段により信頼できないと判定された通信装置との通信を禁止する通信制御手段

と、を備える。

【0027】

【発明の実施の形態】

以下、本発明に係る近接通信装置、携帯端末、近接通信装置を制御するプログラム及び携帯端末を制御するプログラムについて図面を参照しながら具体的に説明する。以下では主に、Bluetooth端末とBluetooth装置との間でBluetoothによる接続を確立し、当該Bluetooth端末を所持するユーザにBluetooth装置が情報を提供する場合を例にとって説明する。

【0028】

図1は本発明に係る情報提供装置の一実施形態であるBluetooth装置1.0の内部構成を示す図である。Bluetooth装置1.0は、バス1に接続されたCPU2、メモリ3、ROM4、記憶装置5、RS-232Cコントローラ6及び有線／無線通信部7と、RS-232Cコントローラ6に接続されたBluetooth送受信部（以下、BT送受信部）8とを有する。

【0029】

BT送受信部8は、Bluetooth携帯端末11との間で、Bluetoothの仕様で通信を行う。Bluetooth携帯端末11に提供する各種の情報は、記憶装置5に格納しておいてもよいし、有線／無線通信部7を介してインターネット9上のサーバに格納しておき、このサーバにアクセスして、Bluetooth携帯端末11から要求のあった情報を取得してもよい。

【0030】

記憶装置5の具体的な形態は特に問わないが、ハードディスク、DVD-RAM、DVD-ROM及び半導体ディスクなどが考えられる。有線／無線通信部7は、有線及び無線のどちらで通信を行ってもよい。有線で通信を行う場合、イーサネット（登録商標）とIPプロトコル、あるいは、電話線、PPP及びIPなどの組み合わせが考えられる。無線で通信を行う場合、無線インターネットを使用するか、携帯電話やPHSのパケット通信を使用してもよい。

【0031】

BT送受信部8は、単にBluetooth送受信用モジュールのみの構成、あるいは、B

T送受信部8に別途CPUやメモリを搭載し、上位のプロトコル、たとえば、L2CAPやRFCOMMなどの処理を行う構成のどちらでもよい。

【0032】

Bluetooth送受信用モジュールのみの構成の場合、仕様書で定義されたHCI(Host Controller Interface)コマンドを送信し、その結果をイベントとして受信する。Bluetoothプロトコルは、利用者へのサービスや情報提供を行うアプリケーションプログラムと共に、CPU2によりメモリ3にロードされ実行される。その他、OS、ドライバ、アプリケーションは、メモリ3に記憶されている。上位のプロトコルの処理を行う構成の場合、実装に依存したコマンドやイベントを使用して、BT送受信部8の制御とデータの送受信を実現する。

なお、BT送受信部8は、必ずしもRS-232Cを介してホストに接続する必要はなく、例えば、ホストの内部バスに直接接続してもよいし、USB(Universal Serial Bus)を介して、接続してもよい。

【0033】

図2は、Bluetooth携帯端末11の内部構成の一例を示すブロック図である。図2のBluetooth携帯端末11は、バス12に接続されたCPU13、メモリ14、ROM15、A/D変換器16、D/A変換器17、偏心モータ18、通信部19、表示部20、キー入力部21、EEPROM22、選択指示部23及びBT送受信部24を有する。A/D変換器16にはマイク25が接続され、D/A変換器17にはスピーカ26が接続されている。通信部19は、有線または無線により基地局27と通信を行う。

【0034】

BT送受信部24は、例えばBluetooth装置10との間で無線通信路を確立し、Bluetooth装置10あるいはインターネット上のサーバに対して情報送信要求コマンドを送信したり、このコマンドに対応する情報を取得したりする。

【0035】

BT送受信部24は、Bluetooth装置10内のBT送受信部8と同様の構成でもよいし、異なる構成でもよい。

【0036】

Bluetooth携帯端末11の音声通話機能は、従来の携帯電話と同様であり、例えば、通信部19は、基地局27との間で位置登録、発呼・着呼時の呼制御を行ってデータの送受信を行い、通信が終了すると切断の呼制御を行い、通信中はハンドオーバ等を行う。

【0037】

通信部19は、基地局27からの接続要求を受信すると、スピーカ26から呼び出し音を出力する。あるいは、偏芯モータ18を駆動させて、Bluetooth携帯端末11の筐体を振動させてユーザの注意を喚起する。ユーザの接続了解指示を受信すると、キャリアは2地点間の回線接続を行い、通信が開始される。

【0038】

Bluetooth携帯端末11は、通信時には、マイク25から入力された音声をA/D変換部16でアナログ信号からデジタル信号に変換し、CPU13の制御の下、デジタルデータの圧縮処理を行い、通信部19を通じて近接の基地局27に送信する。また、通信部19で受信された信号は、CPU13の制御の下、伸張処理等を施されて元の信号に戻され、D/A変換部17でデジタル信号からアナログ信号に変換され、スピーカ26から出力される。

【0039】

CPU13、メモリ14、ROM15、表示部20、キー入力部21、EEPROM22及び選択指示部23は、主に通話以外の目的、すなわち各種情報処理を行う等のために設けられる。例えば、CPU13は、制御プログラムやアプリケーションプログラムの実行を行う。メモリ14は一時的な変数や作業データなどを格納する。ROM15はプログラムや辞書データを記憶する。表示部20はメニューやデータなどを表示する。キー入力部21は、電話番号、数字及び文字などを入力する。EEPROM22は個人登録情報などを保存する。選択指示部23は、メニュー等の選択を行う。

【0040】

BT送受信部24から取得した情報は、そのまま、あるいは表示用のフォーマットに変換されて、表示部20に表示される。

【0041】

図3はBluetooth携帯端末11の情報取得方法を示すフローチャートである。まず、通信可能な相手装置を発見するインクワイアリを実行する（ステップS21）。インクワイアリを行う側（この場合、Bluetooth携帯端末11）はマスター、インクワイアリスキャンを行う側（この場合、Bluetooth装置10）はスレーブと呼ばれる。インクワイアリスキャン状態に設定されたBluetooth装置10のみがBluetooth携帯端末11からのインクワイアリに返答する。

【0042】

Bluetooth携帯端末11は、インクワイアリを行うために、IQパケットを通常10秒間周囲にブロードキャストする（ステップS2-2）。IQパケットにはIAC(Inquiry Access Code)が含まれており、このコードを使用してすべての、あるいは、特定のデバイス（Bluetooth装置10）の発見を行う。自装置に関連するIACを含むIQパケットを受信したBluetooth装置10は、ランダムに決められた時間待機後、再度IQパケットを受信すると、自装置のBluetoothアドレス、クロック、デバイスクラスなどの属性をBluetooth携帯端末11に返信する。

【0043】

Bluetooth携帯端末11は、各Bluetooth装置10からの返信を受け取ると（ステップS2-3）、FHSパケットの含まれたBluetooth装置10のBluetoothアドレス、クロック及びCODを取得し（ステップS2-4）、あらかじめCODが指定されているのであれば、指定されたCODを持つBluetoothアドレスのみ一時的にメモリ14のリストに記録する（ステップS2-5, S2-6）。

【0044】

決められた時間インクワイアリを行うと、インクワイアリ完了イベントを受信する。このイベントを受信すると、Bluetooth装置10が見つかった否かを判定し（ステップS2-7）、見つからなかった場合はその旨を表示する（ステップS2-8）。見つかった場合は、メモリ14のリストに先ほど記録したBluetoothアドレスを持つBluetooth装置10に対して、利用者の装置識別に役立つリモートネーム取得コマンドを送信する。このとき、先ほど取得したBluetooth装置10のクロック情報を用いると、取得時間を短縮することができる。

【0045】

リストに記録したBluetooth装置10からリモートネームの要求に対する返信を受信すると（ステップS29）、その結果を先ほど取得したBluetoothアドレス、クロック、デバイスクラスと合わせて記録しておき（ステップS30）、その結果を表示部20に提示する（ステップS31, S32）。

【0046】

利用者はその中から所望の装置を選択し、対応するBluetoothアドレスを取得して、その装置に対して接続要求を行う（ステップS33, S34）。セキュリティを有している場合は、認証用のリンクキーの入力、あるいは、リンクキーを作成するためのPINコードを入力が求められる。適切な値を設定すると、マスターとスレーブ間でデータ通信用のリンクが確立する（ステップS35）。リンク確立後、関連するプロファイル間での接続が行われて通信が可能となる。リンクが確立しなければ接続エラー表示を行う（ステップS36）。

【0047】

リンクが確立すると、上位プロトコルで接続し（ステップS37）、情報の取得要求を送信すると（ステップS38）、情報を取得して（ステップS39）、情報を表示する（ステップS40）。

【0048】

Bluetooth装置10が自装置内の記憶装置5に保存された情報を提供する場合には、オブジェクト・プッシュ・プロファイルやファイル転送プロファイルが用いられ、L2CAP、RFCOMM、FTPプロトコルが使用される。有線／無線通信部7を用いてインターネット上の情報にアクセスする場合は、ダイアルアップ・プロファイルやPANプロファイルが用いられ、ダイアルアップ・プロファイルにはL2CAP、RFCOMM、PPP、IP、HTTPプロトコルが使用され、PNAプロファイルにはL2CAP、イーサエミュレーション、IP及びHTTPプロトコルが使用される。FTPによりBluetooth装置10から取得した情報や、HTTPによりインターネット上のサーバから取得した情報は、そのまま、あるいは表示用に整形して表示される。

【0049】

次に、情報提供を行うBluetooth装置10の処理手順を説明する。まず、Bluetooth装置10の製造組立て時に接続情報を自装置内部に記録しておく実施形態に

について説明する。

【0050】

図4はサービス提供を行う前のBluetooth装置10の準備作業を示すフローチャートである。仮に、Bluetooth装置10の6バイトであるBTアドレスを「012345ABCDEF」の12文字で表現し、Bluetooth装置10が提供するサービスあるいは情報を表すサービス名称を「浜松町駅周辺案内情報」の10文字で表現するものとする（ステップS51）。前者をBTアドレス文字、後者をサービス名称文字と定義する。

【0051】

これら2つの文字をあわせた22文字のデータは、1文字2バイトデータで表現されるため、全体で44バイト、352ビットのサイズになる。これをBTアドレス付きサービス名称文字と定義する（ステップS52）。

【0052】

この352ビットのデータに対してハッシュ演算を行い、128ビットのハッシュ値を得る（ステップS53）。計算した128ビットのハッシュ値に対して、あらかじめ準備された秘密鍵を用いて128ビットの暗号化データを求める（ステップS54）。ハッシュ値の計算にはMD5、暗号化にはラインデール方式が利用できる。これらは1例であって128ビットのデータが扱える他の方式でも同等の効果を得られる。暗号鍵は128ビット以外のものも使用可能であり、鍵長により、計算時間とセキュリティ強度のトレードオフとなる。

【0053】

暗号化された16バイト128ビットのデータを32文字のデータに変換する、例えば、「0A4F5G……59EF」とする。BTアドレス付きサービス名称文字と変換されたデータを合わせたものを認証文字と定義する（ステップS55）。この例では、認証文字は、「浜松町駅周辺案内情報012345ABCDEF0A4F5G……59EF」となる。

【0054】

次に、サービス名称の文字の長さを「010」の3文字で表現し、これをサービス名称長さ文字と定義する（ステップS56）。3文字のサービス名称長さ文字

、10文字のサービス名称文字、32文字の認証文字をあわせた45文字を認証付きサービス名称文字と定義する（ステップS57）。この例では、認証付きサービス名称文字は、「010浜松町駅周辺案内情報012345ABCDEF0A4F5G……59EF」となる。

【0055】

また、処理を高速化するために頭に識別文字、例えば、2文字の「!!」を挿入したものをBluetooth装置10の装置識別情報と定義する（ステップS58）。この例では「!!010浜松町駅周辺案内情報012345ABCDEF0A4F5G……59EF」となる。

【0056】

なお、上述した識別文字中の各文字の配置方法は一例であり、他の配置方法でも同等の効果が得られる。また、バイナリーデータの変換を単純に2バイトコードで処理しているが、UUENCODEと呼ばれる変換方式では、変換後のデータのサイズをもとの3分の4程度に抑えることができる。

【0057】

上記処理を秘密鍵管理で安全に行うには、セキュリティ性の高い装置でBluetooth装置10ごとにBluetooth装置10の装置識別情報を計算し、作成されたBluetooth装置10の装置識別情報を、各Bluetooth装置10の記憶装置5に記録しておく（ステップS59）。また、秘密鍵とCODの値を情報取得JAVA（登録商標）アプリケーションの初期データとして作成し（ステップS60）、JAVAプログラムとあわせてインターネット上のサーバを通じて利用者に配布する（ステップS61）。情報取得を望む利用者は、公衆網を通じて特定のサーバにアクセスを行い（ステップS62）、JAVAアプリケーションをダウンロードし、自端末に保存しておき、情報を取得する時にJAVAアプリケーションを使用する（ステップS63）。

【0058】

秘密鍵はJAVAプログラムとともにあわせて配布してもよい、あるいは、あとで説明するがBluetooth装置10で秘密鍵をセキュアに管理できる場合は、定期的にJAVAアプリケーションが専用のサーバに取得することにより更新することも可

能である。

【0059】

次に、Bluetooth装置10のサービス提供時の処理を説明する。図5はBluetooth装置10のサービス提供時の処理手順を示すフローチャートである。情報提供を行うBluetooth装置10の電源投入時に、必要なプログラムが記憶装置5からメモリ3に読み込まれ、情報提供を実現するアプリケーションが動作を開始する（ステップS71）。アプリケーションは、利用者の所持するBluetooth携帯端末11との接続を実現するためにBT送受信部8の制御とBluetoothプロトコルを実現するスタックを実行する（ステップS72）。

【0060】

アプリケーションは、まずBT送受信部8に対してリセットコマンドを送信する（ステップS73）。次に、アプリケーションは、Bluetooth装置10の装置識別情報を、他装置からリモートネーム取得コマンドで取得可能な自装置のローカルネームに設定する（ステップS74）。次に、アプリケーションは、CODデバイスをオブジェクト送信系、あるいは、インフォメーション系として設定する（ステップS75）。

【0061】

その後、インクワイアリスキャンとページスキャンを有効とすることで（ステップS76）、Bluetooth携帯端末11からの接続待ち状態となる（ステップS77）。Bluetooth携帯端末11が接続すると（ステップS78）、インクワイアリスキャンとページスキャンを無効にし（ステップS79）、接続したBluetooth携帯端末11に対してサービスを提供し（ステップS80）、サービス提供が完了すると、接続を切断する（ステップS81）。

【0062】

次に、Bluetooth携帯端末11の動作を説明する。図6はBluetooth携帯端末11の処理手順を示すフローチャートである。情報取得を目的とする利用者は、専用のJAVAアプリケーションの起動を指示し、Bluetooth装置10の探索を指示する（ステップS91）。JAVAアプリケーションは、BT送受信部24に対してインクワイアリコマンド送信を要求する。この探索は、所定時間（例えば、10秒間

) 行われる（ステップS92）。

【0063】

BT送受信部24は、発見したBluetooth装置10のアドレス、CODをJAVAアプリケーションにイベントとして通知する（ステップS93）。JAVAアプリケーションは、通知により特定の関数をコールし、CODの検査を行う（ステップS94）。BT送受信部24は、あらかじめ定めたCODとの比較を行い（ステップS95）、一致した場合のみ、そのBluetooth装置10のBluetoothアドレスを検査対象リストに加える（ステップS96）。

【0064】

BT送受信部24は、一定期間経過するとインクワイアリを中止し、インクワイアリ完了イベントをアプリケーションに通知する。アプリケーションは、インクワイアリ完了イベントを受信すると、検査対象リストに記録されているBluetooth装置10が存在するか否かを判定し（ステップS97）、存在しなければ、端末なしを表示する（ステップS98）。

【0065】

検査対象リストに記録されているBluetooth装置10が存在すれば、そのリストに記録した各装置10に対して順番にリモートネーム取得コマンドを送信するようBT送受信部24に指示し（ステップS99）、各Bluetooth装置10が正しい装置か否かを検証した結果をフラグとして記録する（ステップS100, S101）。リモートネームの取得と検証をリストに記録した端末の数だけ繰り返し（ステップS102）、各装置が信頼できるかどうか個別に判定を行う。

【0066】

すべての検査対象のBluetooth装置が信頼できるかどうかを判定するフラグを検査し、信頼できる装置の場合は、そのサービス名称をサービス提供装置の候補として画面に表示する（ステップS103）。信頼できない装置の場合は、画面に表示しない、あるいは、信頼できる装置とは区別できる形式で表示する。信頼できない装置を表示する／しないは、利用者が別途設定できるようにする。また区別する方法としては、異なる色で表示する、イタリックの書体を用いる、マークをつけるなどが考えられる。

【0067】

また、利用者が信頼できないBluetooth装置10への接続要求を行った場合は、利用者に検証できない装置であることを提示して、接続の確認を行う（ステップS104）。

【0068】

次に、図6のステップS100の検証の手順を図7のフローチャートを用いて詳しく説明する。最初に検証用のデータの取得方法、次に取得したデータを持った検証方法を説明する。

【0069】

BT送受信部24は、通信相手のBluetooth装置10のBluetoothアドレスを読み出して（ステップS111）、リモートネームを取得すると（ステップS112）、JAVAアプリケーションに通知する。JAVAアプリケーションは、取得したリモートネームのデータを検査する。

【0070】

JAVAアプリケーションは、最初に取得したリモートネームの最初の数文字が識別文字か否かを判定する（ステップS113）。この場合は、「!!」である。識別文字と一致しない場合は、検査対象のBluetooth装置10のBluetoothアドレスと該当しないことを示すフラグを対にしてメモリ14に記録し、次のBluetooth装置10のリモートネームを取得する。

【0071】

識別文字と一致した場合は、3文字目（バイナリデータで計算すると6バイト）から3文字（バイナリデータでは6バイト）「010」を切り出し、そのデータをサービス名称長さ文字であると解釈し、文字数字データ変換を行いサービス名称の長さを得る（ステップS114）。

【0072】

変換時にエラーが生じた場合は、検査対象のBluetooth装置10のBluetoothアドレスと該当しないことを示すフラグを対にしてメモリ14に記録し、次のBluetooth装置10のリモートネームを取得する。

【0073】

数字に変換できた場合は、取得した長さの分6文字目から、この例では10文字分の文字「浜松町駅周辺案内情報」をサービス名として取得する（ステップS115）。6文字+サービス名称文字の長さ+1、この場合16文字目から12文字をBTアドレス文字として取得し、6バイトのBluetoothアドレスに変換して（ステップS116）、リモートネームの取得を行ったBluetooth装置10のアドレスとの比較を行う（ステップS117）。

【0074】

アドレスが一致しない場合は、検査対象のBluetooth装置10のBluetoothアドレスと該当しないことを示すフラグを対にしてメモリ14に記録し、次のBluetooth装置10のリモートネームを取得する。

【0075】

ステップS117でアドレスが一致した場合は、28文字目から残りの文字のサイズが32文字かどうか検査し（ステップS118）、32文字である場合は、認証用のデータとして取得し、取得した文字データを16バイトのバイナリデータに変換する（ステップS119）。

【0076】

サービス名称の長さ分のサービス名が取得できない場合、BTアドレス文字が6バイトのBluetoothアドレスに変換できない場合、残りの文字が32文字と異なる場合、認証用データが数字に変換できない場合は、検査対象のBluetooth装置10のBluetoothアドレスと該当しないことを示すフラグを対にしてメモリ14に記録し、次のBluetooth装置10のリモートネームを取得する。

【0077】

ステップS119でバイナリデータに変換できた場合は、上記手順でリモートネームから取得したサービス名称と認証用データを用いて端末の認証を行う。

【0078】

リモートネームを取得したBluetooth装置10のBTアドレスを、「012345ABCDE
F」の12文字の文字データに変換する（ステップS120）。サービス名称文字とあわせた22文字のデータは、1文字2バイトデータで表現されるため、全体で44バイト、352ビットのサイズになる（ステップS121）。この35

2ビットのデータに対してハッシュ演算を行い128ビットのハッシュ値を得る（ステップS122）。

【0079】

取得した認証用データをあらかじめ準備された秘密鍵を用いて復号し、128ビットのハッシュ値を求める。この値と先ほど計算したハッシュ値を比較する（ステップS123）。相手が正しい秘密鍵を所持していれば、この値は一致し、一致したことを示すフラグを設定する（ステップS124）。秘密鍵が異なれば、復号化されたデータも異なるためハッシュ値は一致しない。一致しない場合は、検査中のBluetooth装置10は、該当しないことを示すフラグをセットし（ステップS125）、次の装置のリモートネームを取得する。

【0080】

悪意ある装置が、正しい装置に設定されたBluetooth装置10の装置識別情報をコピーしても正しい装置と悪意ある装置のBluetoothアドレスが異なるため、ハッシュ値は一致しない。それゆえ、不正な装置を検出することが可能となる。

【0081】

本実施形態では、双方共通の鍵を使用したが、公開鍵を使用しても同等の効果が得られる。Bluetooth装置10の装置識別情報を作成するときは、秘密鍵を使用し、JAVAアプリケーションには秘密鍵に対応する公開鍵を含めて配布しても同等の効果が得られる。

【0082】

上記実施形態では、Bluetooth装置10の装置識別情報をあらかじめBluetooth装置10に記録してあるが、Bluetooth装置10が他の通信手段を有する場合は、その通信手段を通じて、定期的、あるいは、必要なときに、異なる秘密鍵で作成したBluetooth装置10の装置識別情報を取得し、Bluetooth装置10の装置識別情報を更新する。あわせて、JAVAアプリケーションも定期的にサーバにアクセスし、共通の秘密鍵を更新することにより、セキュリティを強化する方法も考えられる。あるいは、Bluetooth装置10が秘密鍵をセキュアに保存できるのであれば、Bluetooth装置10自身で、定期的に、あるいは、必要な時にBluetooth装置10の装置識別情報を更新することができる。

【0083】

また、ハッシュ値を作成する場合、双方秘密のデータを含めて作成することにより、セキュリティを強化する形態もありうる。

【0084】

公開鍵を使用し、Bluetooth装置10がBluetooth装置10の装置識別情報を更新する場合は、Bluetooth装置10のBTアドレスを含めず、時刻などの情報を交わりに用いることでも同等の効果が得られる。

【0085】

あるいは、Bluetooth装置10の装置識別情報に識別情報の有効期限を含めることにより、携帯端末はその有効期限を検査することにより、さらなるセキュリティの強化を行うことが可能となる。

【0086】

また、OBEXなどの上位プロトコル接続のために、サービス情報取得プロトコルを実行して、接続に必要な情報の取得を行うが、あらかじめ、Bluetooth装置10の装置識別情報に接続情報を含めることにより、サービス情報取得のための通信を省くことが可能となり、処理時間の短縮を行うことが可能となる。

【0087】

Bluetooth携帯端末11において、処理を早まるために、信頼できないと判定したBluetooth装置10のアドレスを信頼できない装置のリストとしてメモリ14に記録しておき、次回から、インクワイアリ終了後、発見したBluetooth装置10のBTアドレスと、信頼できない装置のリストを比較し、その装置が信頼できないと判定した場合には、その装置を検査対象のリストに含めないことにより、全体の処理速度を向上させることが可能となる。

【0088】

このように、本実施形態では、Bluetooth装置10の装置識別情報を、サービス名称、BTアドレス及び暗号化データで構成するため、この装置識別情報を受け取ったBluetooth携帯端末11は接続しようとするBluetooth装置10が信頼できるか否かを正確に判断でき、不正な装置との通信を回避でき、セキュリティ性を向上できる。

【0089】

上述した実施形態で説明した図4～図7の処理は、ハードウェアで構成してもよいし、ソフトウェアで構成してもよい。ソフトウェアで構成する場合には、図4～図7の処理を実行するプログラムをフロッピーディスクやCD-ROM等の記録媒体に収納し、コンピュータに読み込ませて実行させてもよい。記録媒体は、磁気ディスクや光ディスク等の携帯可能なものに限定されず、ハードディスク装置やメモリなどの固定型の記録媒体でもよい。

【0090】

また、図4～図7の処理を実行するプログラムを、インターネット等の通信回線（無線通信も含む）を介して発布してもよい。さらに、同プログラムを暗号化したり、変調をかけたり、圧縮した状態で、インターネット等の有線回線や無線回線を介して、あるいは記録媒体に収納して発布してもよい。

【0091】

なお、本発明は、上記の実施形態に限定されるものではなく、実施段階ではその要旨を逸脱しない範囲で種々に変形することが可能である。さらに、上記実施形態には種々の段階の発明は含まれており、開示される複数の構成用件における適宜な組み合わせにより、種々の発明が抽出され得る。例えば、実施形態に示される全構成要件から幾つかの構成要件が削除されても、発明が解決しようとする課題の欄で述べた課題（の少なくとも1つ）が解決でき、発明の効果の欄で述べられている効果（のなくとも1つ）が得られる場合には、この構成要件が削除された構成が発明として抽出され得る。

【0092】**【発明の効果】**

以上詳細に説明したように、本発明によれば、サービス名称と装置識別情報を含む第1識別情報を暗号化した暗号化データを生成し、サービス名称、装置識別情報及び暗号化データを含む第2識別情報を他の通信装置に送信するため、通信相手が信頼できるか否かを正確に判断でき、不正な装置との通信を回避でき、セキュリティ性能の向上が図れる。

【図面の簡単な説明】

【図1】

本発明に係る情報提供装置の一実施形態であるBluetooth装置10の内部構成を示す図。

【図2】

Bluetooth携帯端末11の内部構成の一例を示すブロック図。

【図3】

Bluetooth携帯端末11の情報取得方法を示すフローチャート。

【図4】

サービス提供を行う前のBluetooth装置10の準備作業を示すフローチャート。

。

【図5】

Bluetooth装置10のサービス提供時の処理手順を示すフローチャート。

【図6】

Bluetooth携帯端末11の処理手順を示すフローチャート。

【図7】

図6のステップS100の検証手順の詳細フローチャート。

【図8】

Bluetooth端末が任意の場所で任意の相手からサービスを受けるための処理手順を示すフローチャート。

【符号の説明】

- 1 バス
- 2 CPU
- 3 メモリ
- 4 ROM
- 5 記憶装置
- 6 RS-232Cコントローラ
- 7 有線／無線通信部
- 8 BT送受信部
- 9 インターネット

1 0 Bluetooth装置

1 1 Bluetooth端末

1 2 バス

1 3 CPU

1 4 メモリ

1 5 ROM

1 6 A/D変換器

1 7 D/A変換器

1 8 偏心モータ

1 9 有線／無線通信部

2 0 表示部

2 1 キー入力部

2 2 EEPROM

2 3 選択指示部

2 4 BT送受信部

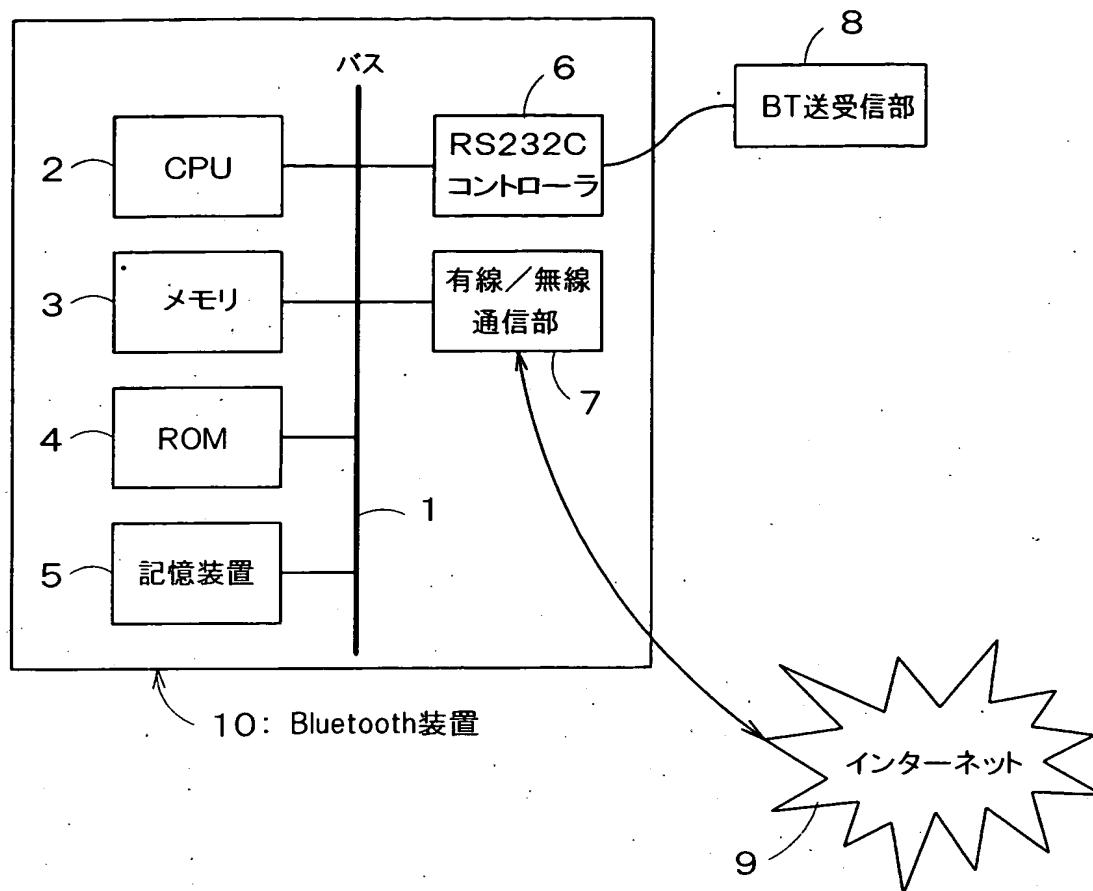
2 5 マイク

2 6 スピーカ

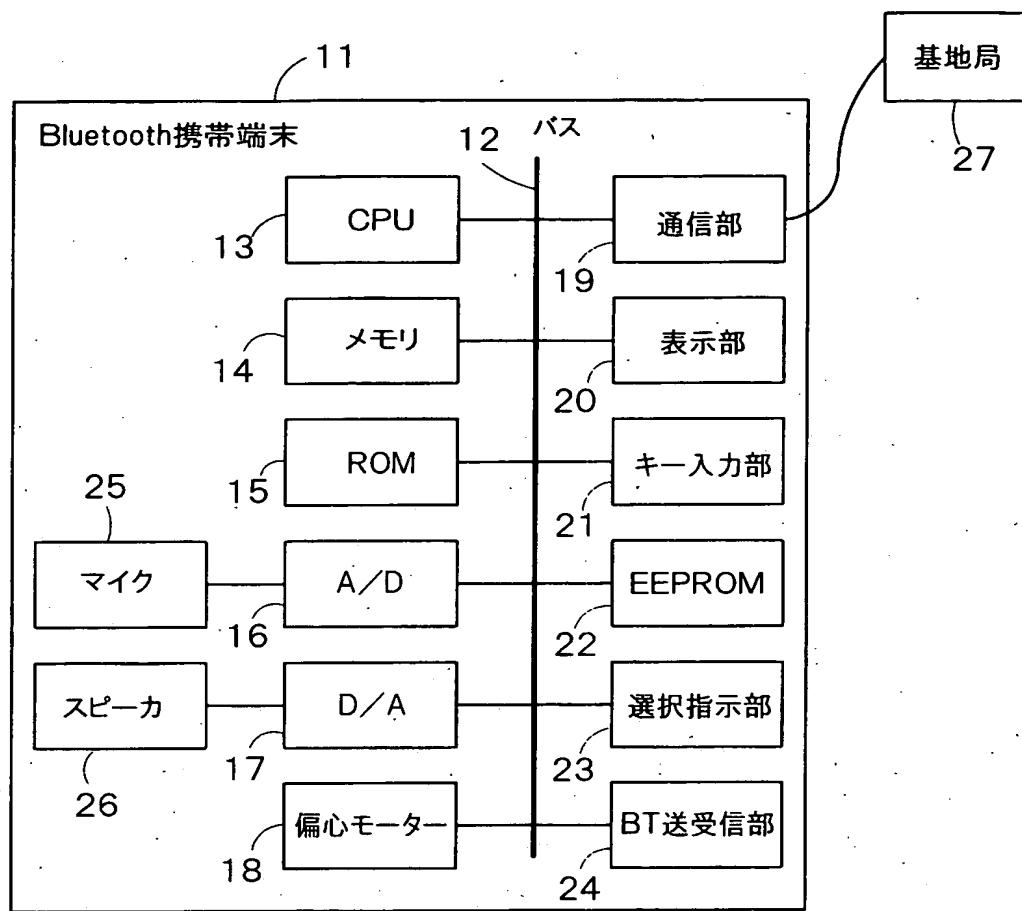
2 7 基地局

【書類名】 図面

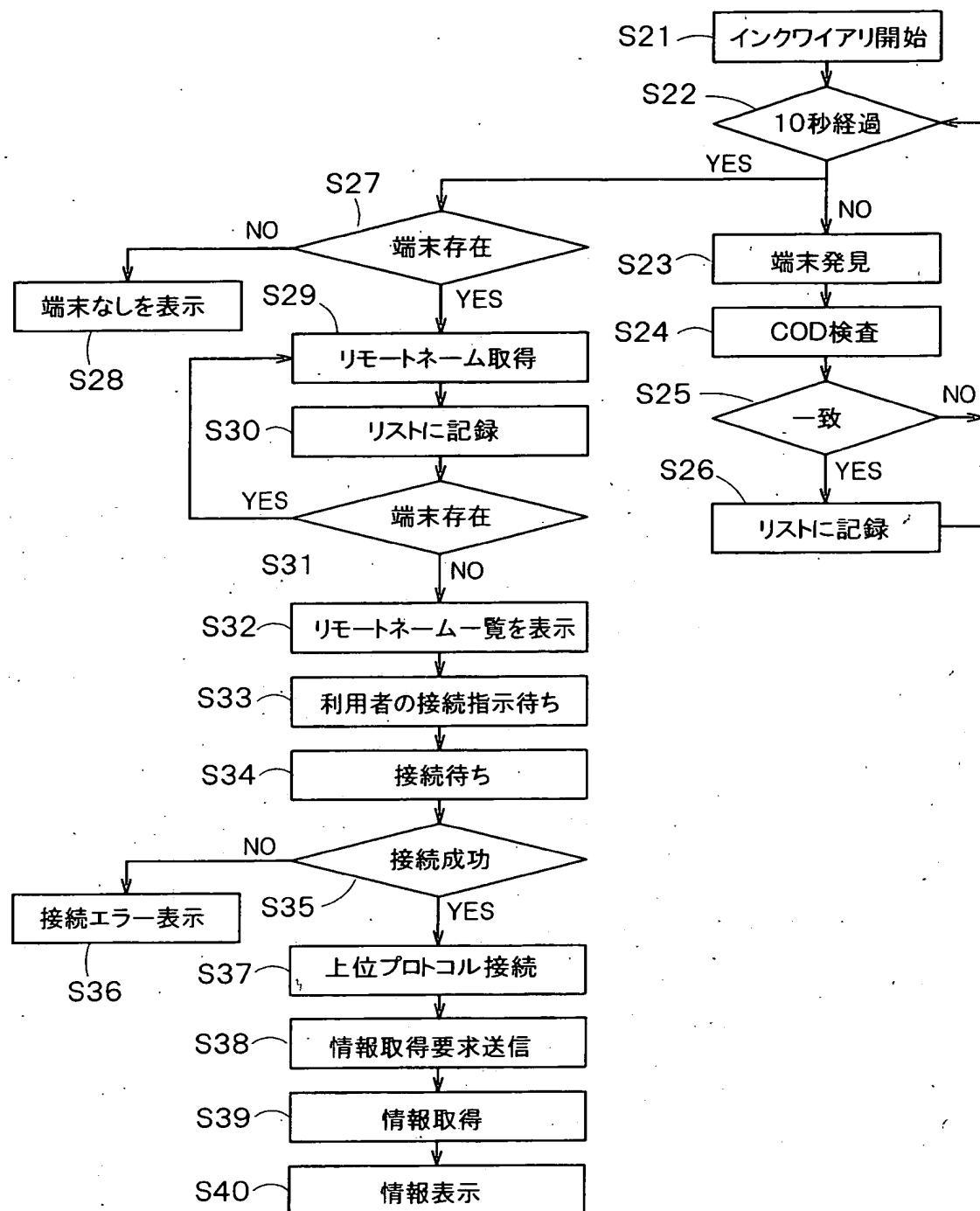
【図1】



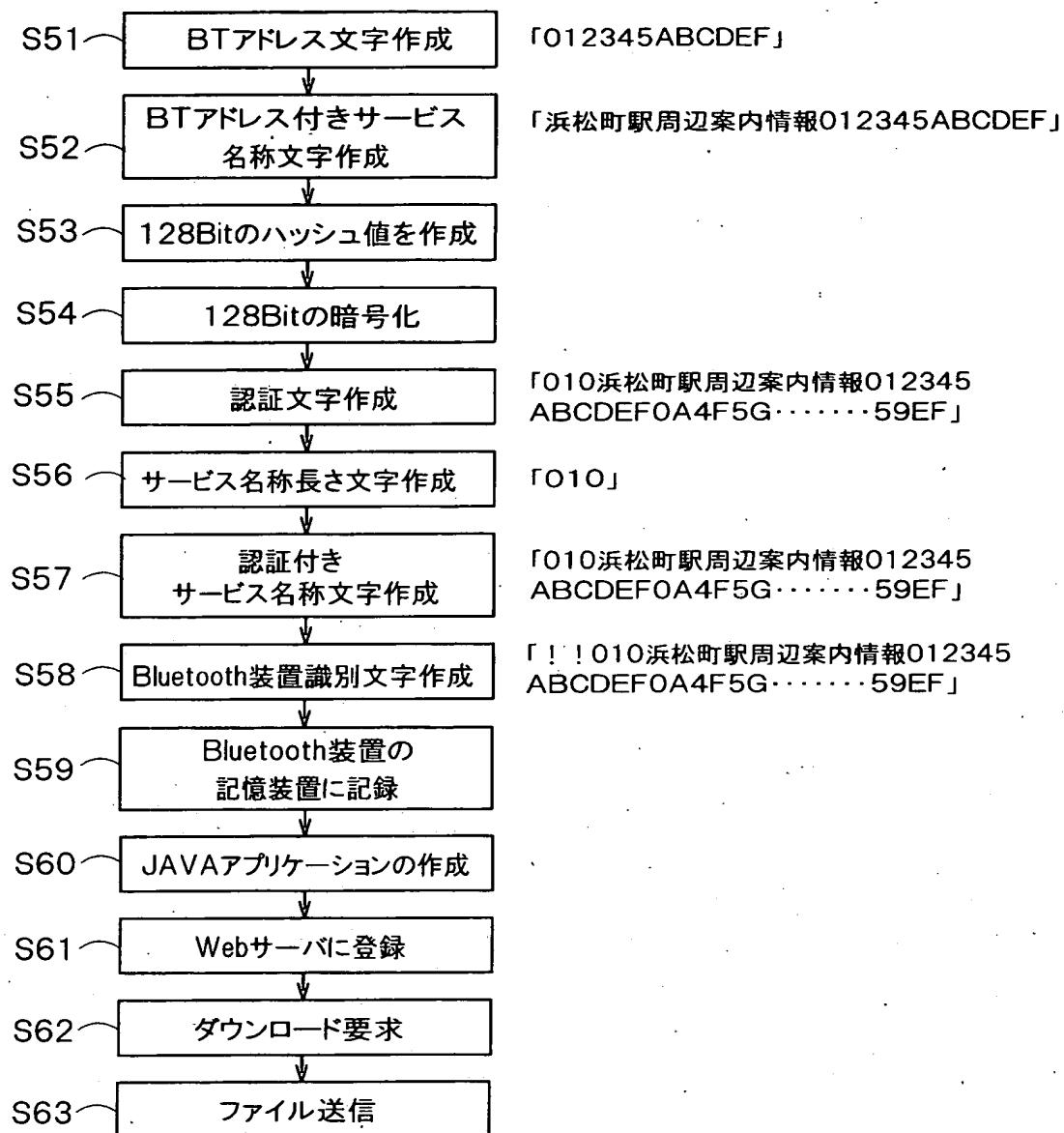
【図2】



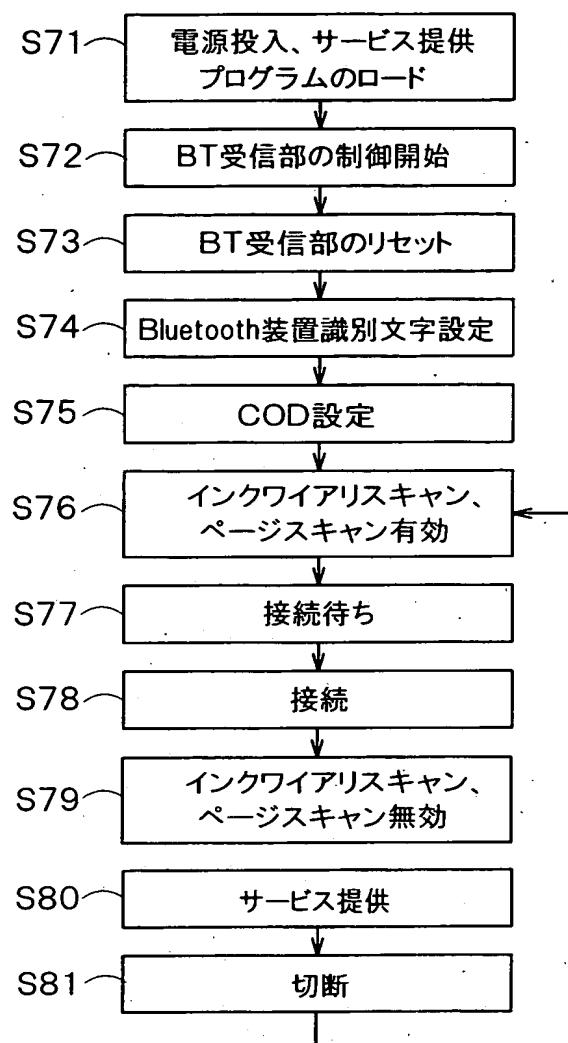
【図3】



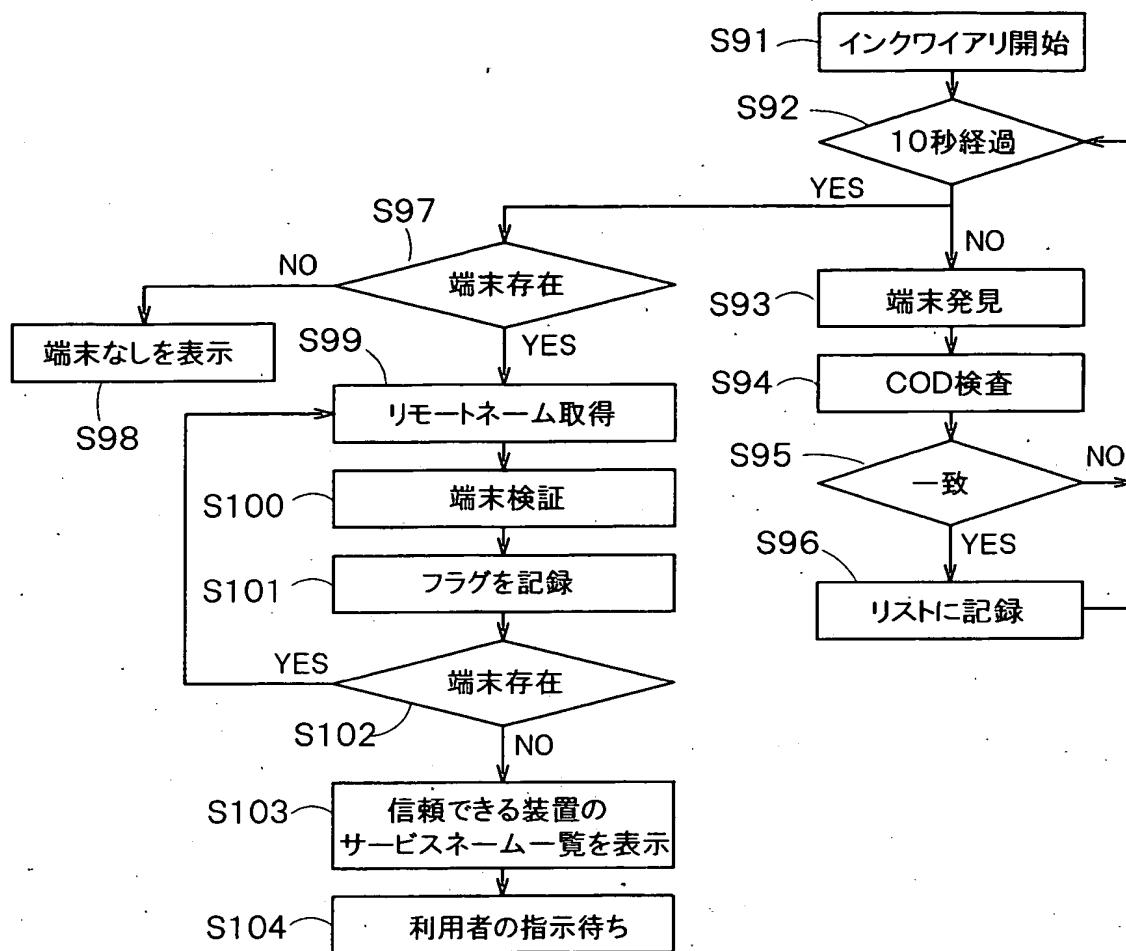
【図4】



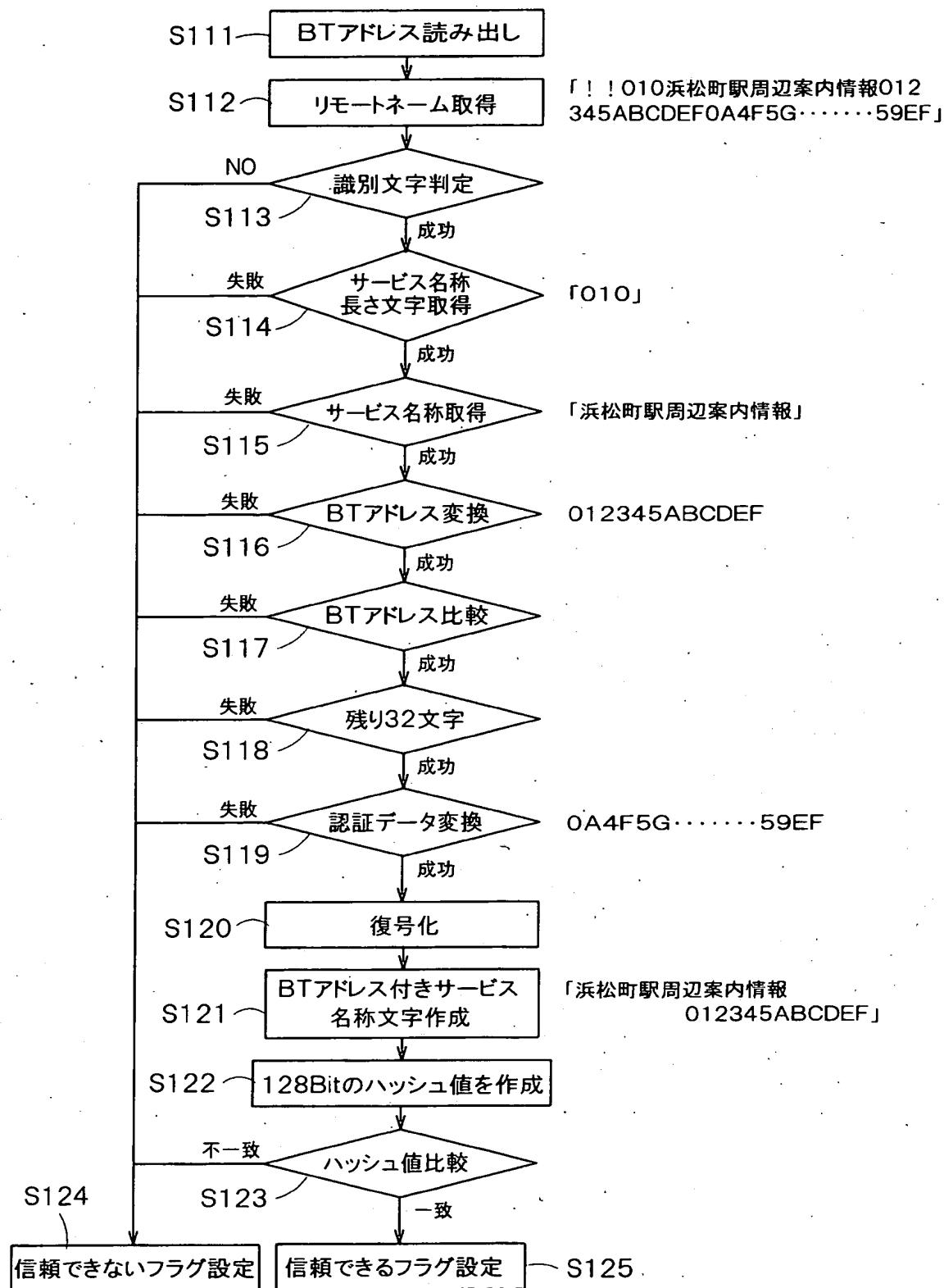
【図 5】



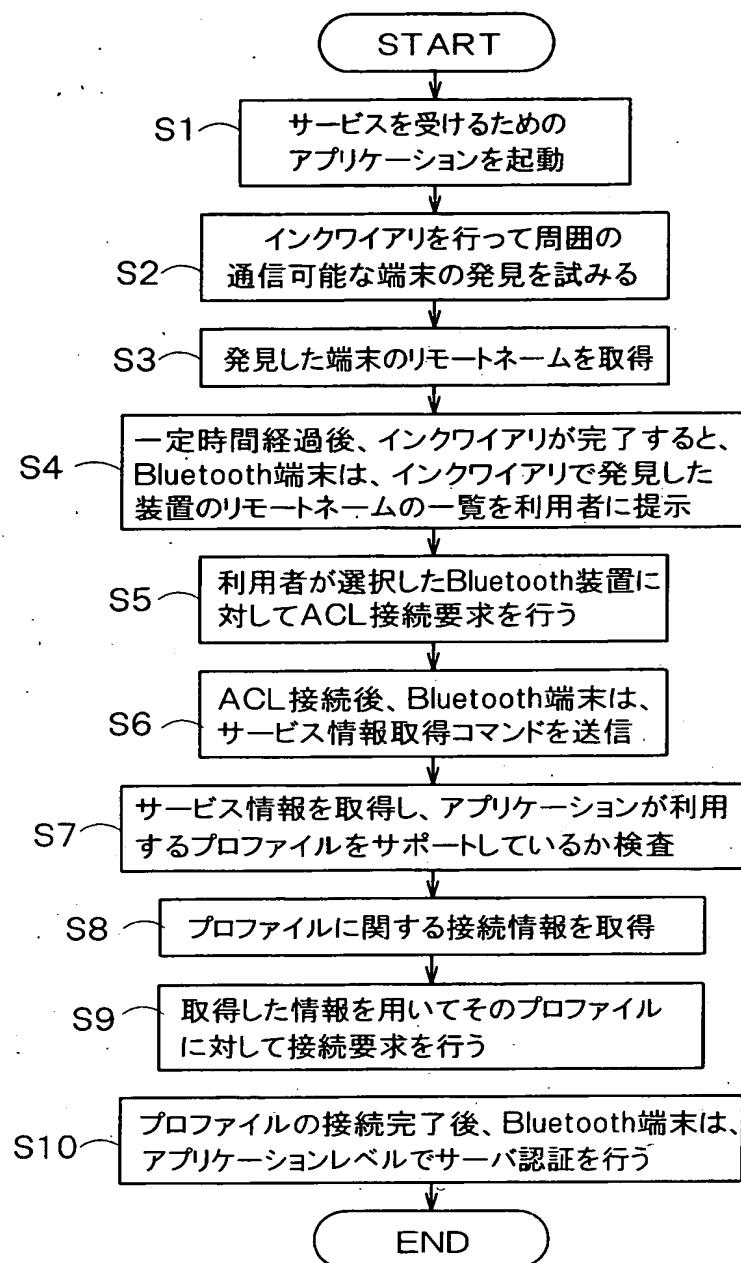
【図6】



【図7】



【図8】



【書類名】 要約書

【要約】

【課題】 信頼できるサービスを提供する通信装置に簡易かつ迅速かつ正しく接続する。

【解決手段】 Bluetooth装置10は、バス1に接続されたCPU2、メモリ3、ROM4、記憶装置5、RS-232Cコントローラ6及び有線／無線通信部7と、RS-232Cコントローラ6に接続されたBT送受信部8とを有する。Bluetooth携帯端末11は、バス12に接続されたCPU13、メモリ14、ROM15、A/D変換器16、D/A変換器17、偏心モータ18、通信部19、表示部20、キー入力部21、EEPROM22、選択指示部23及びBT送受信部24を有する。Bluetooth装置10の装置識別情報を、サービス名称、BTアドレス及び暗号化データで構成するため、この装置識別情報を受け取ったBluetooth携帯端末11は接続しようとするBluetooth装置10が信頼できるか否かを正確に判断でき、不正な装置との通信を回避でき、セキュリティ性を向上できる。

【選択図】 図1

特願2002-321348

出願人履歴情報

識別番号 [000003078]

1. 変更年月日 2001年 7月 2日
[変更理由] 住所変更
住 所 東京都港区芝浦一丁目1番1号
氏 名 株式会社東芝

2. 変更年月日 2003年 5月 9日
[変更理由] 名称変更
住 所 住所変更
氏 名 東京都港区芝浦一丁目1番1号
株式会社東芝